UNITED STATES DISTRICT COURT
FOR DISTRICT OF MASSACHUSETTS

DAVID HOUSE, Plaintiff, v. JANET NAPOLITANO, in her official capacity as Secretary of the U.S. Department of Homeland Security; ALAN BERSIN, in his official capacity as Commissioner, U.S. Customs and Border Protection; JOHN T. MORTON, in his official capacity as Assistant Secretary of Homeland Security for U.S. Immigration and Customs Enforcement, Defendants.	Case No. 1:11-cv-10852-DJC

PLAINTIFF'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS, OR IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Rules

INTRODUCTION

The question in this case is whether the government can, without any suspicion, take an American's electronic devices from him at the border, keep them for 49 days in order to make copies, retain the copied information indefinitely, examine and analyze the information, and share that information with other parts of the federal government and potentially with foreign governments as well. The government does not contest that this is what happened to Plaintiff David House when he crossed the border on his way home from vacation in November 2010, or that he was targeted because of his lawful associational activities. The government asks this Court to dismiss this case, arguing that neither the Fourth Amendment's prohibition on unreasonable searches and seizures nor the First Amendment's protections for expressive records and association pose a bar to these actions because its power to search electronic devices is without limit and effectively beyond judicial review. It sees no difference between going through someone's most private papers and examining their shoes and contact lens solution, and asserts it is free to take people's property from them at the border and hold onto it for weeks, months, or even years, if that is how long, in its view, it would take to conduct a search. It also asks in the alternative that this Court grant it summary judgment on Plaintiff's claim that the government violated his constitutional rights by seizing the device for 49 days, offering a litany of excuses for the delay.

This Court should hold that Plaintiff stated a claim because the government violated his Fourth and First Amendment rights by searching his electronic devices and and seizing his laptop, USB drive, and camera and not returning them for 49 days without reasonable suspicion. While the Court need not reach Defendants' summary judgment claims, if it does, it should deny summary judgment because the government's justifications for the delay are disputed.

FACTUAL SETTING

I. The Formation Of The Bradley Manning Support Network And The Targeting Of David House By The United States Government

David House and others joined together in June 2010 to organize political support for the defense of Bradley Manning, a U.S. serviceman deployed in Iraq who was arrested in May 2010 on suspicion of having disclosed restricted material to WikiLeaks. Compl. ¶¶ 9, 12, May 13, 2011, ECF No. 1. Manning's arrest followed WikiLeaks' publication of "Collateral Murder," a video of U.S. forces killing Iraqi civilians during a 2007 air attack in Baghdad. *Id.* ¶ 10. In July 2010, Manning was formally charged with accessing and disclosing classified information without authorization, including "a classified video of a military operation" and fifty State Department cables. *Id.* ¶ 9. Authorities brought further charges against him in March 2011, including a charge that he knowingly gave intelligence to the enemy – a capital offense. *Id.* Following his arrest, Manning was moved to a military detention facility in Quantico, Virginia, where he was held until April 2011 in solitary confinement under conditions that have been widely criticized as degrading and humiliating. *Id.* Both Manning's alleged disclosure of government records and the suspected connection between Manning and WikiLeaks are the subjects of ongoing criminal investigations. *Id.* ¶ 11.[1]

The Bradley Manning Support Network ("Support Network"), formed by Mr. House and others, is an unincorporated association of individuals and organizations and describes itself as an "international grassroots effort to help accused whistle blower Pfc. Bradley Manning." *Id.* ¶ 12. Its stated purposes include: harnessing the outrage of viewers of "Collateral Murder" for a coordinated effort in defense of Manning; coordinating international support for Manning;

[1] The Defense Department has acknowledged that the investigation of Manning by the U.S. Army Criminal Investigation Command is ongoing. Compl. ¶ 11. The disclosure of classified information is also the subject of an ongoing investigation by the Justice Department and a federal grand jury sitting in the Eastern District of Virginia. *Id.*

raising funds for Manning's legal defense; and providing support for Manning during his imprisonment. *Id.* The Support Network pursues these objectives through its website and internet presence, the organization of public events, and private contacts with individuals. *Id.* The Support Network is not affiliated with WikiLeaks. *Id.*

In addition to his role as a founding member of the Support Network, Mr. House, a computer programmer and researcher, developed the organization's website. *Id.* ¶¶ 12-13. He currently serves on the Support Network's Steering Committee, is active in its work, and regularly communicates with others who are concerned about Manning's treatment and prosecution. *Id.* ¶13. He has also served as one of the organization's primary fundraisers and in that capacity has been responsible for meeting potential supporters and soliciting donations for Manning's legal defense. *Id.*

Although the work of the Support Network, including that of Mr. House, consists solely of lawful activity, Mr. House became a target of federal investigators following the organization's establishment. *Id.* ¶ 14. He has been visited and questioned, both at his home and at his place of work, by investigators for the Department of Defense, the Department of State, and the Federal Bureau of Investigation. *Id.* Mr. House has also been the subject of ongoing surveillance. *Id.* He has been placed on a watch list, which results in his being stopped for questioning and searched by authorities each time he enters the United States. Decl. of David House ("House Decl.") ¶ 5, Sept. 19, 2011 (Pls.' Statement of Material Facts Ex. 1). Since September 2010, Mr. House has been detained at the border on every occasion in which he has re-entered the United States after foreign travel, and he has been questioned about his work with the Support Network or political beliefs. Compl. ¶ 14.

II. The November 3, 2010 Seizure Of David House's Electronic Devices

On November 3, 2010, following a vacation in Mexico, Mr. House arrived at the Chicago O'Hare International Airport, where he planned to catch a connecting flight to Boston. Compl. ¶ 15. As the plane arrived at O'Hare, an announcement was made that everyone should have their passports out to be checked by government officials on the jetway as they deplaned.[2] House Decl. ¶ 4. Leaving the plane, Mr. House observed two uniformed agents taking people's passports, checking them, and giving them back. *Id.* When Plaintiff handed his passport to the agents, they checked it, looked at each other, and handed it back to him. *Id.* The agents then turned around and left the jetway, neglecting to check the documentation of the passengers deplaning after him. *Id.*

Mr. House then proceeded through a passport control station and was admitted for entry into the United States as a U.S. citizen. Compl. ¶ 15; House Decl. ¶ 5. He was referred to secondary screening, where his belongings (and those of a traveling companion) were searched by a Customs and Border Patrol Agent. Compl. ¶ 15; House Decl. ¶ 5. Mr. House was then questioned about whether he had been using his computer. Compl. ¶ 15; House Decl. ¶ 5. After he had been told that he was free to go, Mr. House was detained by Special Agents Louck and Santiago. Compl. ¶¶ 15-16; House Decl. ¶¶ 4-6. The agents stated that they were with the Department of Homeland Security ("DHS") and told Mr. House that he was being detained and would have to give them any electronic devices he was carrying. Compl. ¶¶ 16-17. Plaintiff surrendered his computer, USB storage device, camera, and cellular phone. *Id.* ¶ 17. The agents did not ask consent for the seizure of the devices, did not present Mr. House with a search warrant, and did not explain the purpose or authority for the seizure. *Id.*

[2] The cursory description provided by Agents Louck and Santiago omits significant details and, to the extent relevant, Plaintiff notes that there are disputes as to the manner in which his electronic devices were seized.

The agents took Mr. House's devices and directed him to sit and wait. *Id.* When the agents returned a short time later, they were no longer in possession of the items they had taken. *Id.* Mr. House was directed to accompany the two agents to an interrogation room, where he was initially asked a series of questions concerning the security of his computer. *Id.* ¶ 18. He advised the agents that the computer's hard disk was not encrypted, but that the computer was password protected. *Id.* When asked, he declined to give them his password, explaining that the password would allow direct and unauthorized access to research on his employer's server. *Id.* Mr. House asked the agents if he was required by law to disclose the password but did not receive a response. House Decl. ¶ 7.

Agents Louck and Santiago detained Mr. House for questioning for an extended period of time. Compl. ¶ 19. They questioned him about his association with Bradley Manning, his work for the Support Network, whether he had any connections to WikiLeaks, and whether he had been in contact with anyone from WikiLeaks during his trip to Mexico. *Id.* Mr. House was asked no questions relating to border control, customs, trade, immigration, or terrorism, and at no point did the agents suggest that Mr. House had broken the law or that his computer contained any illegal material. *Id.*

When Mr. House was finally allowed to leave, the agents returned only his cellular phone. *Id.* ¶ 20. The other items that had been taken, specifically his laptop, USB device, and camera, were not returned. *Id.* Mr. House was given a receipt listing the items that had been seized, indicating that "R. Hart, SAC CHI ICE" had taken custody of them, and was told that they would be returned by FedEx within a week. *Id.* On December 21, 2010, 48 days after the agents seized Mr. House's electronic devices, they remained in government custody. *Id.* ¶ 21. On that date, Mr. House, through counsel, sent a letter by facsimile to the Department of

Homeland Security ("DHS"), Customs and Border Protection ("CBP"), and Immigration and Customs Enforcement ("ICE") requesting that his electronic devices be returned to him immediately. *Id.* He also requested documentation of the chain of custody of any copies made of the information contained on his devices and documentation of their destruction. *Id.*

On December 22, 2010, Mr. House received his electronic devices by mail from the "DHS CIS New York District Office." *Id.* ¶ 22. In a letter to Mr. House's counsel dated December 30, 2010, general counsel for ICE noted that the devices had been returned but did not indicate whether any information derived from those devices had been copied, what agencies or individuals were given any copies made, or whether any such copies had been destroyed. *Id.* ¶ 23.

III. The Search, Retention, And Dissemination Of The Expressive And Privileged Contents Of Mr. House's Electronic Devices

Defendants have reviewed and copied the contents of Mr. House's electronic devices and this information has been retained by ICE. Decl. of Robert Marten, Defs.' Concise Statement of Material Facts Pursuant to Local Rule 56.1 ("Defs.' Facts"), Ex. 4, ¶¶ 7, 15, July 27, 2011, ECF No. 12-1. The information has also been shared with, and retained by, other government agencies. Compl. ¶ 27.[3]

The continued search, retention, and distribution of Mr. House's information are expressly authorized by ICE policy. A border search policy issued by ICE in August 2009 permits border officials to read and analyze information on international travelers' electronic devices without reasonable suspicion. U.S. Immigration and Customs Enforcement, "Border

[3] The declarations submitted by Defendants have not addressed whether ICE obtained technical assistance from another agency or whether information obtained from Mr. House's devices was shared with other agencies or individuals.

Searches of Electronic Devices," Directive No. 7-6.1, § 6.1, Defs.' Facts, Ex. 5, Aug. 18, 2009, ECF No. 12-1.[4]

The policy also permits border officials to read and analyze, even without reasonable suspicion, privileged or other sensitive information. *Id.* § 8.6(1). The policy provides that sensitive information shall be handled in accordance with "all applicable federal law and ICE policy." *Id.* § 8.6(2)(c). The policy does not, however, specify any law or policy that might require reasonable suspicion, and the policy itself contains no such requirement.

The policy permits border officials, without any suspicion of wrongdoing, to detain a traveler's electronic devices, or the information they contain, for further reading, scrutiny, and copying after the traveler has left the border and even for a potentially unlimited time. *Id.* § 8.1(4). The policy specifies that travelers' devices or the information they contain may also be removed from the border port and sent elsewhere. *Id.* The policy does not explain or limit where travelers' devices or information may be sent. The policy does not place time limits on how long ICE may detain a traveler's devices, retain the information they contain, or continue to read and analyze the information. While the policy provides for intermittent supervisory approvals as a detention continues, it also provides for limitless extensions. *Id.* § 8.3. At no point during a potentially limitless detention and search period is there a requirement of reasonable suspicion. The policy also permits border officials to share devices or the information they contain with other agencies, still absent reasonable suspicion, in order to obtain "technical assistance." *Id.* § 8.4(1).

[4] The border search policy issued by CBP in August 2009, CBP, "Border Search of Electronic Devices Containing Information," Directive No. 3340-049, Defs.' Facts Ex. 6, Aug. 20, 2009, is substantially similar to the ICE Policy.

Not only can ICE search and detain a traveler's electronic devices without reasonable suspicion, but it, along with other federal agencies and state, local, and foreign governments, can also permanently retain travelers' information. ICE may retain information relating to immigration, customs, and other enforcement matters obtained from a search of an electronic device, even without probable cause. *Id.* § 8.5(1)(b). Once information is permanently retained, nothing in the policies limits its authority to share that information. *Id.* § 8.5(1)(c). Also, agencies that obtain information as part of a request for technical assistance may retain it on their own authority. *Id.* § 8.5(2)(c).

IV. Expressive And Privileged Contents Of Mr. House's Electronic Devices

Mr. House's computer and other electronic devices contained private and sensitive materials that he did not intend to expose to view by others without his consent, including personal and private information and information concerning his work on behalf of the Support Network. Compl. ¶ 28. The devices contained his personal e-mail communications covering a period of several years, including messages sent to and from family members and friends and concerning employment related matters, records of his personal finances, computer programming works in progress, and passwords allowing access to his bank account, to his workplace computer, and to secure communications websites. *Id.* ¶ 29. Moreover, the devices contained information concerning the Support Network, including the complete Support Network mailing list, confidential communications between members of the Steering Committee about strategy and fund-raising activities, the identity of donors, lists of potential donors and their ability to contribute, and notes on meetings with donors including personal observations about those donors. *Id.* ¶ 30.

The privacy of certain information concerning the operation and supporters of the Support Network that has been accessed, retained, and shared by Defendants is essential to the

effective operation of the organization. *Id.* ¶ 32. The seizure and retention of this information and its dissemination to other governments, agencies, private entities, individuals, or the public at large will chill the associational rights of the Bradley Manning Support Network and its supporters, including Mr. House, by exposing them to harassment or reprisals, by deterring open discussion of political strategy, and by causing the withdrawal of lawful support and deterring such support. *Id.* ¶ 33. The Manning prosecution is a highly charged and politically controversial issue. The President of the United States has publicly commented on the case, stating that Manning has broken the law. Manning and his supporters, along with WikiLeaks, have been criticized for posing a threat to national security and have been accused by some of treason. Furthermore, Mr. House and other individuals who have publicly supported Manning have been identified by name and targeted for retaliation. *Id.* ¶ 34. Because some supporters and contributors to the Support Network will contribute to the Manning defense or otherwise support the Support Network's work only if they can remain anonymous, the retention, disclosure, and/or use by Defendants and other government agencies of information concerning the identity of individual supporters and donors and of potential supporters and donors will materially interfere with lawful activities and association in support of Manning's defense. *Id.* ¶ 35.

ARGUMENT

I. DEFENDANTS' ACTIONS VIOLATED THE FOURTH AMENDMENT.

Defendants wrongly contend that they have unreviewable discretion to search the personal papers on individuals' electronic devices and to seize these devices for as long as they like. There are three reasons why a search of an electronic device triggers a reasonable suspicion requirement: it is non-routine, it is particularly offensive, and it imposes a serious burden on First Amendment activity. The length of time the government took Plaintiff's electronic devices

also provides an independent basis for finding a Fourth Amendment violation. Computers are not like socks or contact lens solution; they are repositories of our intimate and private personal papers, not just those needed for one trip but a complete archive of our thoughts for many years. The doctrines Defendants lean on, such as the closed container doctrine, were developed in a different time and in another context.

To be sure, the two circuits to consider whether suspicion is needed for laptop searches have concluded that none is necessary, but other judges have disagreed for compelling reasons. *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005); *see also United States v. Linarez-Delgado*, 259 Fed. Appx. 508 (3d Cir. 2007) (reaching same conclusion as to video footage). As Judge Kozinski has written, suspicionless searches of personal papers at the border runs counter to the "[f]ounders' deep concern with safeguarding the privacy of thoughts and ideas-what we might call freedom of conscience-from invasion by the government." *United States v. Seljan*, 547 F.3d 993, 1014 (9th Cir. 2008) (Kozinski, J. dissenting). He explained, "[w]hat makes papers special-and the reason they are listed alongside houses, persons and effects-is the ideas they embody, ideas that can only be seized by reading the words on the page." *Id.* at 1017. Although the Ninth Circuit became the first circuit to authorize a detention of a laptop without reasonable suspicion, *United States v. Cotterman*, 637 F.3d 1068 (9th Cir. 2011), it did so over the forceful dissent of Judge Betty Fletcher, who explained how "seizing one's personal property deprives the individual of his valid possessory interest in his property," and "authorizing a generalized computer forensic search (untethered to any particularized suspicion) permits the government to engage in the type of generalized fishing expeditions that the Fourth Amendment is designed to prevent." *Id.* at 1084.

A. The Suspicionless Search Of Mr. House's Electronic Devices Violated His Fourth Amendment Rights.

Plaintiff has alleged that Defendants had no reasonable suspicion to search his electronic devices and Defendants do not suggest otherwise. Thus, this Court must accept Plaintiff's assertion that Defendants searched Plaintiff's laptop without suspicion. Compl. ¶ 31; Fed. R. Civ. P. 8(b)(6). The Fourth Amendment prohibits the government from searching the contents of Mr. House's electronic devices at the border absent reasonable suspicion, for three reasons.[5] First, because of their invasive nature, searches of electronic devices are "non-routine" searches that require reasonable suspicion. Second, suspicionless electronic device searches are unreasonable because of the "particularly offensive manner" in which they are carried out. Finally, because electronic device searches involve searches of First Amendment-protected material, the reasonable suspicion standard is the constitutional minimum.

1. The Search Of Mr. House's Electronic Devices Was Not Routine.

The border is not a Fourth Amendment-free zone. Although the Supreme Court has found that the government has broad powers to conduct searches at the border, *see United States v. Ramsey*, 431 U.S. 606, 616 (1977), it has also recognized that "non-routine" border searches require at least reasonable suspicion of wrongdoing, *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985). The First Circuit has held that when deciding whether a search is non-routine, the determining factor is "[t]he degree of invasiveness or intrusiveness." *United States v. Braks*, 842 F.2d 509, 511 (1st Cir. 1988). The uniquely private and vast amount of information stored on electronic devices renders searches of these devices highly invasive.

[5] Plaintiff does not contest Defendants' assertion that the initial search and detention of his electronic devices occurred at the border or the functional equivalent thereof. *See* Defs.' Br. 9-10.

A search of an electronic device intrudes upon a traveler's dignity and privacy. With each passing day, people conduct and store more of their lives on computers, smart phones, and other electronic devices. These devices are far more than receptacles for private files; they have become a commonplace part of the daily life of the average person. They are constantly used to help people think, learn, communicate, associate with others, and keep track of their own lives and those of their families. *See generally* Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 Widener L.J. 667 (2006). A consequence of this new reality is that these devices also maintain a nearly indelible record of everything their users think or search for, what they learn or read, what they say to others, and with whom they associate. The information stored on Mr. House's computer, for example, spanned a period of years and included emails "sent to and from family members and friends and messages concerning employment related matters, records of his personal finances, computer programming work in progress, and passwords allowing access to his bank account, his workplace computer, and secure communications websites." Compl. ¶ 29. His computer also contained information concerning the Support Network, including the complete Support Network mailing list, confidential communications between members of the Steering Committee about strategy and fund-raising activities, the identity of donors, lists of potential donors and their ability to contribute, and notes on meetings with donors including personal observations about those donors. Compl. ¶ 30. Given the nature of information commonly stored on computers, it should come as no surprise that "for most people, their computers are their most private spaces." *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting).

Electronic devices are the gateway to the Internet and all it has to offer, including means of communication such as e-mail, instant messaging, and social networks. As the Sixth Circuit recently noted in holding that individuals have a right to privacy in email:

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities. Much hinges, therefore, on whether the government is permitted [access to] a subscriber's emails without triggering the machinery of the Fourth Amendment.

United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010). Suspicionless searches of electronic devices that facilitate, record, and store such communications undoubtedly implicate heightened concerns of privacy and dignity that distinguish the devices from other types of property that travelers may carry across the border.

The vast quantity of information contained on electronic devices magnifies the privacy and dignity concerns implicated by a border search. A computer "is akin to a vast warehouse of information," and a typical hard drive sold in 2005 can carry data "roughly equivalent to forty million pages of text—about the amount of information contained in the books on one floor of a typical academic library." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1175 (9th Cir. 2010) ("[E]ven inexpensive electronic storage media today can store the equivalent of millions of pages of information."). Such a vast quantity and variety of information increases the likelihood that highly personal information will also be searched, seized, or copied. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 104

(1994). As a consequence, individuals' privacy and dignity interests in the contents of their laptops and similar electronic devices more closely resemble the heightened interests associated with private dwelling areas and should be treated accordingly. *Cf. United States v. Cardona-Sandoval*, 6 F.3d 15, 21-23 (1st Cir. 1993) (distinguishing between an individual's private space and communal public areas of a vessel in analyzing reasonableness of search at sea); *United States v. Whitted*, 541 F.3d 480, 489 (3d Cir. 2008) (requiring suspicion for a border search of a passenger cabin in a vessel); *United States v. Alfonso*, 759 F.2d 728, 738 (9th Cir. 1985) (finding that a border search of the private living quarters on a ship "should require something more than naked suspicion").

Defendants attempt to minimize the privacy interests at stake by arguing, sweepingly, that a border search is always routine unless it involves an invasive bodily search. Mem. Supporting Defs.' Mot. to Dismiss or in the Alternative for Summ. J. ("Defs.' Br.") 11. That is not the law. The First Circuit has explicitly rejected the hard-and-fast distinction that Defendants seek to draw between searches of persons and searches of objects. The court has held that the relevant inquiry in categorizing a search as routine or non-routine is not "whether the precise object of the routine search in question is an individual's person, or instead his luggage and effects, his automobile, etc.," but rather the degree of invasiveness of the search. *Braks*, 842 F.2d at 511 n.5 (construing *Ramsey*, 431 U.S. at 616-619; *Almeida-Sanchez v. United States*, 413 U.S. 266, 272-73 (1973)).[6] The uniquely private and vast quantity of information contained in Mr. House's electronic devices renders the search of those devices highly invasive and therefore

[6] The First Circuit in *Braks* highlighted a number of factors for determining the degree of invasiveness involved in a particular search, but expressly recognized them as non-exhaustive and warned that a border search cannot be categorized as routine or non-routine "merely by stacking up and comparing the several factors favoring each of the two classifications." 842 F.2d at 513.

non-routine. The subsequent case of *United States v. Flores-Montano*, 541 U.S. 149 (2004), does not alter this outcome. Defendants seize on *Flores-Montano* to suggest, incorrectly, that if the search of a vehicle's fuel tank does not implicate the same dignity and privacy interests as an intrusive search of the person, then there must be no property search capable of implicating those interests. Defs.' Br. 11. But the Court in *Flores-Montano* specifically limited its holding to vehicles. It certainly did not hold that all property searches are routine or that they are categorically incapable of implicating the "dignity and privacy interests of the person being searched." 541 U.S. at 152; *see also Whitted*, 541 F.3d at 489; *Alfonso*, 759 F.2d at 738.

Defendants also wrongly rely on the closed container doctrine for support, likening laptops to luggage. Defs.' Br. 11-15. Laptops are not like luggage. While both are capable of storing personal items, the similarity stops there. Far from a glorified suitcase, a personal computer is a revolutionary and indispensible communications tool, allowing users to instantly exchange ideas via e-mail, instant messenger services, blogs, chat rooms, and social networks. It is also the interface that allows people to read and publish information on the Internet covering a range of topics "as diverse as human thought." *Reno v. ACLU*, 521 U.S. 844, 863 (1997) (The Internet is "the most participatory form of mass speech yet developed, . . . entitled to the highest protection from governmental intrusion.") (internal quotation marks and citations omitted). Any comparison to a mere closed container vastly oversimplifies a computer's functions and simply ignores the realities of modern existence.

Defendants place similarly misguided reliance on overly broad and unsupported claims about the practical consequences of applying the reasonable suspicion requirement to border searches of electronic devices. Contrary to Defendants' contention, there is nothing complicated or unduly restrictive in that requirement. Defendants quote from *Montoya de Hernandez* to warn

against "complex balancing test[s]," Defs.' Br. 16, but the context of the quoted language makes clear that the Court in that case was warning against the creation of a *new* Fourth Amendment reasonableness standard, *see Montoya de Hernandez*, 473 U.S. at 541 ("We do not think that the Fourth Amendment's emphasis upon reasonableness is consistent with the creation of a third verbal standard in addition to "reasonable suspicion" and "probable cause . . . ."). The reasonable suspicion standard is not novel. It is a longstanding and familiar standard that, as Defendants acknowledge, border agents already apply in cases of personally invasive searches. *See* Defs.' Br. 11. Moreover, the vast number of cases finding reasonable suspicion to justify border searches of electronic devices belies Defendants' suggestion that applying the standard would thwart border agents' ability to effectively police the borders. *See, e.g., United States v. Irving*, 452 F.3d 110, 124 (2d Cir. 2006); *United States v. Roberts*, 274 F.3d 1007, 1012 (5th Cir. 2001); *United States v. Bunty*, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008); *United States v. Hampe*, No. 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007), *aff'd* No. CR-07-3-B-W, 2007 WL 1806671 (D. Me. June 19, 2007); *United States v. Furukawa*, No. 06-145 (DSD/AJB), 2006 WL 3330726, at *2 (D. Minn. Nov. 16, 2006); *cf. Whitted*, 541 F.3d. at 489 ("Reasonable suspicion is not a high standard that will prevent customs officers from detecting drug smugglers at our borders.").

2. The Search Of Mr. House's Electronic Devices Was Particularly Offensive In Manner.

In *Ramsey*, the Supreme Court stated that a border search may be constitutionally objectionable "because of the particularly offensive manner in which it is carried out." 431 U.S. at 618 n.13. Citing to cases in which the Court had limited the extent to which the government could conduct broad-ranging searches or seizures incident to arrest, the Court suggested that the

offensiveness of the execution of a search may violate the Constitution. *Id.* Laptop searches are similarly offensive in manner.

As described above, electronic devices contain vast quantities of deeply personal and sensitive information. Several federal courts have recognized that because electronic device searches risk devolving into exploratory rummaging through this personal and sensitive information, judicial officers must engage in "greater vigilance . . . in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures." *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1177 (upholding ex ante limits on the execution of warrants to search electronic devices); *accord United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 958-59 (N.D. Ill. 2004); *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998). Although these cases did not involve border searches, they are informed by the very Fourth Amendment concerns about fishing expeditions that the *Ramsey* Court warned might render a border search unreasonable. Defendants' claim of authority to roam through Mr. House's electronic devices without reasonable suspicion must fail.

3. The Search Of Mr. House's Electronic Devices Burdened His Expressive And Associational Interests.

Electronic device searches invariably involve examining an extensive amount of expressive and associational material, and the search of Mr. House's electronic devices was no exception. *See* Compl. ¶¶ 28-30. When a search or seizure burdens First Amendment interests, those interests must be considered in determining whether the search or seizure is reasonable. Because they implicate expressive and associational interests, conducting searches and seizures of electronic devices in the absence of suspicion is unreasonable and violates the Fourth Amendment.

Not all searches and seizures are the same; "[a] seizure reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material." *Roaden v. Kentucky*, 413 U.S. 496, 501 (1973). As *Roaden* held, seizures of expressive materials, such as "books and movie films," are "to be distinguished from" seizures of "instruments of a crime" or "contraband" in appraising reasonableness. *Id.* at 502 (quotation marks omitted). Examining reasonableness "in the light of the values of freedom of expression," the Court required police to obtain a warrant to seize expressive materials even though one would not otherwise have been required. *Id.* at 504. Courts have held that associational material is likewise entitled to heightened procedural protections. *See, e.g., NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460-61 (1958).

Searches that implicate First Amendment-protected materials therefore require the application of heightened Fourth Amendment requirements, up through and including a warrant and probable cause, even where those requirements might not otherwise apply. *Roaden* at 501-04; *see also Maryland v. Macon*, 472 U.S. 463, 468 (1985) ("First Amendment imposes special constraints on searches for and seizures of presumptively protected material.").[7] Relatedly, the Fourth Amendment's procedural protections must be applied with "scrupulous exactitude" when a search implicates expressive materials. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Stanford v. Texas*, 379 U.S. 476, 485 (1965). Because searching electronic devices implicates expressive and associational interests, more procedural protections are required than may typically apply to unprotected materials searched at the border. While these cases did not

[7] To be clear, the meaning of the *probable cause* requirement remains the same whether or not a search targets expressive materials. *New York v. P.J. Video, Inc.*, 475 U.S. 868, 873-75 & n.6 (1986). But as the cases cited in this paragraph make clear, where a search and seizure burdens First Amendment interests, those interests must be taken into account in determining what protections are necessary to make the search reasonable.

involve the border, the Supreme Court has repeatedly rejected the proposition that the border is a Fourth Amendment-free zone, *see, e.g.*, *Montoya de Hernandez*, 473 U.S. at 537-38, and has suggested that government intrusions that implicate expressive conduct, even at the border, should be policed especially carefully by courts, *see, e.g.*, *Ramsey*, 431 U.S. at 624 n.18 (suggesting that "full panoply of Fourth Amendment requirements" might be applicable where government searches implicate expressive rights or threaten to "chill" expressive conduct (citing, *inter alia*, *Roaden* and *Stanford*)).[8] In short, searching electronic devices is different than searching ordinary luggage, and Mr. House did not lose his right to privacy in expressive and associational materials simply because he crossed the border. *Cf. Lamont v. Postmaster Gen.*, 381 U.S. 301, 305 (1965) (holding that restrictions on unfettered delivery of mail from abroad infringed addressees' First Amendment rights).

B. The 49-Day Seizure Of Mr. House's Electronic Devices Violated His Fourth Amendment Rights.

This Court should further hold that Defendants' 49-day seizure of Mr. House's laptop computer, USB storage device, and camera violated his Fourth Amendment rights. Even if no reasonable suspicion was required for the initial seizure, the government cannot deprive a person of his personal property for 49 days, frustrating his privacy and possessory interests in that property, without reasonable suspicion that a search will turn up evidence of a crime. Moreover, the length of the government's seizure must be commensurate with its need, and 49 days is, on

[8] Defendants argue, incorrectly, that application of the reasonable suspicion requirement to border searches of electronic devices would "mean that a traveler's privacy in their personal information would depend on whether the data is reproduced with ink and paper or stored in a computer…." Defs.' Br. 15. Plaintiff does not, however, concede that border officials may in fact conduct suspicionless searches of items such as sealed letters and locked diaries. Several cases call into doubt Defendants' asserted authority to do so. *See, e.g.*, *Ramsey*, 431 U.S. at 618 n.13; *see also United States v. Emery*, 541 F.2d 887, 889 (1st Cir. 1976) (suggesting a difference, even at the border, between expressive materials and packages containing goods).

its face, too long. To the extent that Defendants purport to justify this incident through declarations, those facts are contested.

1. A 49-Day Seizure Of An Electronic Device At The International Border Requires Reasonable Suspicion.

The government cannot seize a traveler's electronic devices for 49 days without reasonable suspicion. Some lower courts have held that as a seizure lengthens in duration the government needs reasonable suspicion or probable cause. *See United States v. Stewart*, 715 F. Supp. 2d 750, 754-55 (E.D. Mich. 2010) (a search of a laptop the day after seizure in a location away from the border required reasonable suspicion because it recognized that "actual dispossession of a traveler's belongings" is a substantial intrusion); *United States v. Laich*, No. 08-20089, 2010 WL 259041, at *1 (E.D. Mich. Jan. 20, 2010) (a permanent seizure of a laptop at the airport, and its transportation hundreds of miles away, required probable cause). Courts of Appeal have also held that as a border detention and search become prolonged, a higher level of suspicion becomes necessary. *See, e.g.*, *United States v. Yang*, 286 F.3d 940, 948 (7th Cir. 2002).

This conclusion makes sense because seizing someone's property is a significant infringement on their possessory interest in that property and can even constrain their liberty interest in continuing with their itinerary. In *United States v. Place*, the Court held that the detention of a domestic traveler's luggage for 90 minutes without probable cause violated the Fourth Amendment. 462 U.S. 696, 699, 708-10 (1983). It reasoned:

> Particularly in the case of detention of luggage within the traveler's immediate possession, the police conduct intrudes on both the suspect's possessory interest in his luggage as well as his liberty interest in proceeding with his itinerary. . . . [S]uch a seizure can effectively restrain the person since he is subjected to the possible disruption of his travel plans in order to remain with his luggage or to arrange for its return.

Id. at 708. The Court held that the length of the detention is "an important factor" in determining what level of suspicion—probable cause or something less—is required. *Id* at 709. Although *Place* involved domestic travel, the Supreme Court has applied the principle that the duration of a seizure ratchets up the level of suspicion required at the international border. *See Montoya de Hernandez*, 473 U.S. at 542-44 (citing *Place* when considering whether a 16-hour border detention could be justified only by reasonable suspicion).

This Court should hold that the government needed reasonable suspicion to seize Mr. House's electronic devices for 49 days. The seizure was a serious interference with Mr. House's possessory interest in his electronic devices, which contained many personal papers. Compl. ¶¶ 28-30. Defendants assert that "there is no *per se* rule limiting the amount of time that the government may expend in pursuit of a lawful border search," Defs.' Br. 2, 19, but, to the contrary, *Place* makes clear that as the duration of a seizure lengthens, the level of suspicion the government must have also increases. A seizure that persists for 49 days triggers a reasonable suspicion requirement.

Defendants' explanation that no reasonable suspicion should be required because searching electronic files "can take a long time" fails to appreciate how seizures burden individuals' privacy and possessory interests. Defs.' Br. 20 (quotation marks omitted). In-depth computer searches take time precisely because they are so invasive, involving numerous unrelated pieces of personal information. *Cf. United States v. Hill*, 459 F.3d 966, 968 (9th Cir. 2006) ("[B]ecause computers typically contain so much information beyond the scope of the criminal investigation, computer-related searches can raise difficult Fourth Amendment issues

different from those encountered when searching paper files."). They invade individuals' privacy and infringe their ability to conduct their livelihoods and communicate with others.[9]

2. The Length Of The Government's Detention Was Not Commensurate With Its Need.

Moreover, this Court should hold that the 49-day seizure violated Mr. House's constitutional rights because its length was not "reasonably related in scope to the circumstances that justified the initial detention at the border." *United States v. Cotterman*, 637 F.3d 1068, 1082 (9th Cir. 2011). In *Cotterman*, a divided panel of the Ninth Circuit rejected the argument that the government needed reasonable suspicion to seize a laptop for two days, but warned that the "Government cannot simply seize property under its border search power and hold it for weeks, months, or years on a whim." *Id.* at 1070. The Fourth Amendment forbids the government from seizing travelers' property for longer than reasonably necessary to effectuate its goals. *Id.* at 1082. The court found that a two-day seizure was reasonable, but only after requiring a full account of what the government was doing with the laptop to ensure that it was acting expeditiously. *Id.* at 1082-83.

There is a remarkable contrast between the full accounting and expeditious actions of the government agents in *Cotterman* and what happened in this case. Defendants seized Plaintiff's electronics on November 3. Marten Decl. ¶ 5. They offer no explanation of where Plaintiff's electronic devices were or what was being done to them between November 3 and November 10. Defendants submitted the affidavit of Robert Marten to explain that ICE spent the time between November 10 and December 17 preparing two certified forensic copies of Plaintiff's devices. Marten Decl. ¶ 7. Marten ascribes the delay solely to problems in making two verified forensic

[9] Defendants additionally explain why it would be impractical to "accept an individual's word for what is located on his or her electronic devices," Defs.' Br. 21, but Plaintiff never argues that they are obligated to do so.

copies of the data contained in Mr. House's computer, citing a variety of technical difficulties and a lack of resource. Marten Decl. ¶¶ 10-13.

Material factual disputes preclude the Court from granting Defendants summary judgment on this ground. Plaintiff's expert attests that the process of imaging and verification described in the Marten declaration should not have taken more than 18 hours, did not require the one week period that the devices were retained by ICE in Chicago, and certainly did not require the period of nearly six weeks that the devices were retained in New York. Decl. of Alexander Stamos ("Stamos Decl.") ¶ 6, Sept. 20, 2011 (Pls.' Statement of Material Facts Ex. 2). Moreover, while Defendants attribute a portion of the delay to the limited number of ICE agents certified in computer forensics and their current workload, Marten Decl. ¶ 13, the declaration is inadequate because it does not explain what portion of the delay was attributable to this factor, does not describe where these agents are located or why the devices were transferred after a week from Chicago to New York, provides no information about any backlog in computer analysis by ICE and whether all computers are detained for a similar period, and does not indicate whether, under ICE Directive 7-6.1, ¶ 8.4, assistance was sought from any other agency.[10]

IV. DEFENDANTS' ACTIONS VIOLATED THE FIRST AMENDMENT.

The government gives short shrift to Plaintiff's First Amendment challenge, stating that a search that satisfies the Fourth Amendment cannot violate the First Amendment. Defs.' Br. 23-24. This is not the law. A border search "can constitute a direct and substantial interference"

[10] Plaintiff believes Defendants' motion for summary judgment should be denied outright but, if this Court is inclined to credit Marten's explanation of lack of resources, it should first allow Plaintiffs to conduct discovery into the many holes in that declaration to gather evidence to support its side of the case. *See* Decl. of John Reinstein ("Reinstein Decl.") ¶ 3, Sept. 20, 2011 (Pls.' Opp'n to Defs. Mot. to Dismiss Ex. 1).

with First Amendment rights. *Tabbaa v. Chertoff*, 509 F.3d 89, 101 (2d Cir. 2007). This is true for electronic device searches, as illustrated by this case.

A. Defendants Have Violated Mr. House's Right To Association.

The government's actions have violated Mr. House's First Amendment right to association. Defendants are now in possession of the complete, confidential list of the Support Network members and supporters, as well as many emails and other documents detailing the Support Network's inner workings. Compl. ¶¶ 28, 30. Nevertheless, citing *Ashcroft v. Iqbal*, 129 S. Ct. 1937 (2009), Defendants seek outright dismissal of Plaintiff's claim that the seizure and dissemination of core organizational material concerning the Support Network violates the right of association guaranteed by the First Amendment. Defs.' Br. 25. Defendants' position oversimplifies the *Iqbal* standard and understates the intrusion on First Amendment rights. As the Court has recently noted, dismissal of a complaint pursuant to Rule 12(b)(6) is inappropriate if properly pleaded allegations of fact state a facially plausible legal claim. *Belyea v. Litton Loan Servicing, LLP*, Civ. Action No. 10-10931-DJC, 2011 WL 2884964, at *1 (D. Mass. July 15, 2011) (citing *Ocasio–Hernández v. Fortuño–Burset*, 640 F.3d 1, 11-12 (1st Cir. 2011)). Plausibility is highly contextual, "dependent on the particular claims asserted, their elements, and the overall factual picture alleged in the complaint." *Chao v. Ballista*, 630 F. Supp. 2d 170, 177 (D. Mass. 2009).

Plaintiff's association claim challenges Defendants' seizure, retention, and dissemination of electronic data concerning the operation and the identity of supporters of the Support Network. Compl. ¶¶ 32-35, 37. It is based on the long-established principles that "[e]ffective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association," *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460

(1958), and that "[a]ccording protection to collective effort on behalf of shared goals is especially important . . . in shielding dissident expression," *Roberts v. U.S. Jaycees*, 468 U.S. 609, 622 (1984). *See also Brown v. Socialist Workers '74 Campaign Comm.*, 459 U.S. 87, 91-93 (1982).

In responding to this claim, Defendants provide the Court with a selective and misleading recitation of the allegations of the complaint which departs from the analysis required by *Iqbal* by removing the search of Plaintiff's devices from the context in which it occurred in order to suggest that any infringement of Plaintiff's right of association "was incidental to a valid exercise of the Government's authority to search and detain personal items at the border." Defs.' Br. 26. The requisite consideration of the context and the overall factual allegations of Plaintiff's complaint present a different picture.

This case arises against the background of the prosecution of Bradley Manning for disclosure of classified information and the efforts to support Manning's defense by those who believe that his conduct was justified by the disclosure of official misconduct and the need for greater transparency. Compl ¶¶ 9-12. The complaint alleges that Plaintiff first attracted the attention of federal agencies after he took an active role in the formation and operation of the Support Network. Compl. ¶ 14. This was first evidenced by investigation by at least three federal agencies and interviews at his home and place of work, where he was questioned about his political activities and beliefs and his visits to Manning at the Quantico detention facility, and by surveillance of his activities. *Id.* The targeting of Mr. House for his associational activity is further evidenced by his placement on the TECS II watch list, which has resulted in his travel

being tracked and in his being subjected to detention and to different and intrusive searches at the border by Defendants' agencies. [11] *Id.*; House Decl. ¶ 5.

The stop of Mr. House on November 3, 2010, moreover, was conducted for the purpose of examining the contents of his computer and investigating his connection with Bradley Manning. At the outset of his detention by Agents Louck and Santiago, whose specific responsibilities on November 3 are notably not described in their declarations, Mr. House was directed to surrender any electronic devices he was carrying. Compl. ¶ 17. He was then detained for an extended period for questioning about his association with Manning and the work of the Support Network. *Id.* ¶ 19. Significantly, he was asked no questions relating to border control, customs, immigration or terrorism. *Id.*

Despite the fact that there appears to have been no been no information obtained from Mr. House's devices that was of relevance to ICE,[12] Plaintiff has alleged that the information was copied and retained by ICE and that it has been disseminated to other government agencies. Compl. ¶ 27. Indeed, Defendants have admitted that ICE has retained a copy of that information, Marten Decl. ¶ 15, but the declarations filed by the government do not address the allegation that the information was shared with and retained by other agencies of the federal government.

---

[11] According to the Treasury Department System of Records Notification required by the Privacy Act of 1974, the description of the routine uses of TECS II includes the following language:

> These records and information in these records may be used to . . . Disclose pertinent information to appropriate Federal, State, local or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

Department of the Treasury, Notice of Privacy Act system of records, 66 Fed. Reg. 52983, 53029 (Oct. 18, 2001).

[12] ICE Directive 8.5(1)(e) provides for destruction of information obtained from electronic devices which is "of no relevance to ICE." Copies of information made by ICE "are only being retained for purposes of litigation." Marten Decl ¶ 15.

Compl. ¶¶ 25-27.[13] That allegation must therefore be taken as true for purposes of Defendants' Rule 12(b)(6) motion.

Finally, the complaint alleges that the data that was copied, shared, and retained contained important and sensitive information about the Support Network including the complete Support Network mailing list, confidential internal communications about strategy and fund raising, the identity of donors and their ability to contribute, and notes on meetings with donors along with personal observations about those donors. Compl. ¶¶ 30, 32. And, Plaintiff has alleged, because there are supporters and donors to Manning's defense who wish to remain anonymous, the seizure of Plaintiff's records by Defendants and the access to that information by other government agencies will deter support for the organization in the future.[14] Compl. ¶ 35.

These allegations fairly meet *Iqbal*'s requirements. Courts have recognized time and again that the harms which Defendants describe as mere "speculation . . . about what [Plaintiff] thinks may happen" are sufficient to establish a burden on fundamental rights. Defs.' Br. 26. "[C]ompelled disclosure, in itself, can seriously infringe on privacy of association and belief guaranteed by the First Amendment." *Buckley v. Valeo*, 424 U.S. 1, 64 (1976). This is obviously true in cases where the threat of imminent harm has been shown on the record, *e.g*, *NAACP v. Alabama*, 357 U.S. at 462; *Bates v. City of Little Rock*, 361 U.S. 516, 521-522 (1960),

[13] Agent Marten's declaration carefully avoids any reference to the involvement of other government agencies and limits discussion of retention of information to "copies ICE made." Marten Decl. ¶ 15.

[14] In the event that the Court finds the language of this allegation to be deficient, Plaintiff requests leave to substitute the following language: "Given the seriousness of the charges in the Manning case, the ongoing criminal investigations by the U.S. Department of Justice involving the publication of government information by WikiLeaks, and the hostility to Manning and WikiLeaks on the part of some organizations and members of the public, a number of individuals have informed me that they will contribute to the Support Network financially or otherwise only if their support can remain anonymous. Several supporters have expressed concern about the seizure of my electronic devices and the information they contained."

but has been recognized as well where the concern was less extensively supported, *e.g.*, *Shelton v. Tucker*, 364 U.S. 479, 485-86 (1960) ("to compel a teacher to disclose his every associational tie is to impair that teacher's right of free association"), and in cases where there has been no record of retaliation, *see Talley v. California*, 362 U.S. 60, 65 (1960) (blanket prohibition of anonymous handbills invalidated because fear of reprisal might deter discussion of public matters); *Pollard v. Roberts*, 283 F. Supp. 248, 258 (E.D. Ark. 1968) (3 judge court), *aff'd per curiam* 393 U.S. 14 (1968) (no evidence that any individuals had been subjected to reprisals on account of support for Republican candidates); *Johnson v. Wash. Times Corp*., 208 F.R.D. 16, 17-18 (D.D.C. 2002) (general claim of bigotry against members of a "controversial" church sufficient).

Defendants' argument to the contrary conflates pleading and proof. Each of the cases cited by Defendants in support of the proposition that there must be "concrete 'harassment and intimidation'" involved the sufficiency of the evidence, not the pleadings. Defs.' Br. 27 (citation omitted); *see Lyng v. Int'l Union*, 485 U.S. 360, 367 n.5 (1988) ("facts . . . do not demonstrate any 'significant' interference"); *In re Motor Fuel Temperature Sales Practices Litig.*, 641 F.3d 470, 490 (10th Cir 2011) (sole evidence of chilling participation in a trade association was minimal and equivocal, consisting only of an unsworn statement); *Doyle v. N.Y. State Div. of Hous. and Cmty. Renewal*, No. 98 CIV. 2161(JGK), 1999 WL 177441, at *7-8 (S.D.N.Y. Mar. 30, 1999) (no evidence presented on summary judgment to support First Amendment claim). By this line of argument, they effectively invite the court to exceed the bounds of *Iqbal* and to resolve contested issues of fact at this preliminary stage.

The Second Circuit's opinion in *Tabbaa*, 509 F.3d at 89, although ultimately resolved in favor the government, supports Plaintiff's position here. The court found that an extended

border stop of individuals returning from an Islamic conference in Canada, involving detention for several hours, questioning, photographing, and fingerprinting, while not exceeding the bounds of a routine search, was sufficient to implicate the protections of the First Amendment because "the prospect of being singled out for such extensive processing could reasonably deter others from associating at similar conferences." *Id.* at 102. The First Amendment claim was rejected only because the government had presented sufficient evidence to establish that it had a compelling interest in preventing terrorists who had attended the conference from entering the United States. *Id*. at 103. Here, however, the government has made no claim that the seizure and retention of information concerning the Support Network was justified for any reason other than the fact that it took place at the border.

B. Defendants Have Violated Mr. House's Right To Free Speech.

Defendants' actions have also violated Mr. House's right to free speech. Because they burden the right to engage in First Amendment activity in private, lower courts have applied heightened scrutiny to efforts to find out what individuals are reading or what movies they are watching. *See, e.g.*, *Amazon.com LLC v. Lay*, No. C10-664 MJP, 2010 WL 4262266, at *10-12 (W.D. Wash. Oct. 25, 2010) (holding that state's request for titles of expressive materials purchased through Amazon.com violated customers' First Amendment rights); *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*, 706 F. Supp. 2d 11, 17-18 (D.D.C. 2009). Just as heightened scrutiny applies to government efforts to compel disclosure of sales records of expressive items and association membership lists, it must apply to government attempts to search individuals' electronic devices, which have the capacity to reveal all this and more.

The government's search of Plaintiff's electronic devices burdened his First Amendment rights because it forced him to reveal to the government his thoughts where those thoughts had previously been shielded from observation. Compl. ¶ 29. Yet the government has failed to put forth any reasons it had to justify a search of Mr. House's personal papers, other than a vague and generalized interest in border security. This interest is not sufficient to satisfy the heightened scrutiny that applies to searches of expressive records.

CONCLUSION

For the foregoing reasons, Defendants' motion should be DENIED.

Respectfully submitted,

DAVID HOUSE
By his attorneys,
/s/ *Catherine Crump*
Catherine Crump, Pro Hac Vice
ccrump@aclu.org
Speech, Privacy and Technology Project
American Civil Liberties Union
125 Broad Street, 17th floor
New York, New York 10004
(212) 549-2500

/s/ *John Reinstein*
John Reinstein, BBO # 416120
jreinstein@aclum.org
Laura Rótolo, BBO # 665247
lrotolo@aclum.org
Alexia De Vincentis, BBO # 679397
adevincentis@aclum.org
American Civil Liberties Union
of Massachusetts
211 Congress Street
Boston, Massachusetts 02110
(617) 482-3170

September 21, 2011

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Catherine Crump
Catherine Crump
September 21, 2011